Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints

Andreas Reinhardt
Department of Informatics
TU Clausthal, Clausthal-Zellerfeld, Germany
andreas.reinhardt@tu-clausthal.de

Georgios Konstantinou
School of Electrical Engineering and Telecommunications
The University of New South Wales, Sydney, Australia
g.konstantinou@unsw.edu.au

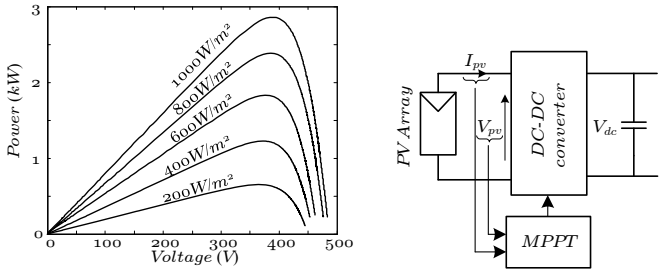
Dominik Egarter
KELAG-Kärntner Elektrizitäts-Aktiengesellschaft
Klagenfurt, Austria
dominik.egarter@kelag.at

Delphine Christin
University of Bonn and
Fraunhofer FKIE, Bonn, Germany
christin@cs.uni-bonn.de

***Abstract*—Solar power has emerged as one of the three most widely installed renewable energy sources around the globe. Photovoltaic (PV) capacity in excess of 150 GW had been installed in 2013 already, and many more installations are connected to worldwide power grids every day; especially in the form of small-scale PV plants in domestic environments. However, in order to connect PV installations to the power grid, their dc output must be converted to the nominal mains voltage and frequency through the use of *converters*. In this paper, we propose a novel approach to influence the maximum power point tracking (MPPT) component of such a PV converter in order to enable two main privacy-preserving operations: Firstly, by deliberately reducing the output power through changing the converter's operating point, appliance operations can be emulated in order to pretend user presence during periods of absence. Secondly, by running the converter below optimum output power, and feeding real-time data of an appliance consumption to the device, it is able to hide the appliance's operation from the household's aggregate consumption. We present simulations results that prove how our modified converter design can hide appliance load signatures as well as how it can be used to emulate appliance signatures to falsely indicate user presence.**

I. Introduction

Striving for sustainability has led to the global installation of renewable power generation [1], mostly based on the conversion of photovoltaic (solar radiation), hydroelectric (water motion), or wind power to electric energy. Domestic photovoltaic installations especially contribute to the sustainable power supply of many countries worldwide, given the simplicity of their installation and their operability without the need for centralized coordination. However, their connection to the power grid is complicated by the intermittent nature of the physical phenomenon underlying PV generation, i.e., solar irradiance, as well as the fact that their output is dc whereas virtually all power grids worldwide are designed to transport ac power. As a consequence of these limitations, conversion devices (*converters* and/or *inverters*) are needed to transform the dc output to the nominal mains voltage and frequency, and thus allow such renewable generation plants to be connected to the power grid.



(a) Power vs. voltage (V_{pv}) curves for different irradiance levels (BP65W module). (b) MPPT to maximize the dc-dc converter's output power.

Fig. 1. Maximum Power Point Tracking (MPPT) is used to control the dc-dc converter such that it outputs maximum power.

The power output of a PV array strongly depends on the solar irradiance level and the temperature of the environment, hence it is generally required to continually adapt the array's operating point such that the output power stays maximal. One main technological foundation for maximizing the output power of a PV array is the use of *Maximum Power Point Tracking* (MPPT). Let us briefly revisit its main principle as follows. Fig. 1a shows the typical relation between PV voltage and output power for different irradiance levels. Upon closer inspection, one can observe that the peak output power is reached at different operating voltages V_{pv} for different levels of irradiance. Adapting the *maximum power point* (MPP) accordingly is thus crucial to maximize the energy transfer and typically performed by dc-dc converters, as shown schematically in Fig. 1b. For this reason, a large number of MPPT algorithms, in both the digital or analog domains and with different complexities, have been proposed in the existing literature [2].

Changing the function of the MPPT component in order to enhance user privacy is the core contribution of this work. It is motivated by the existing research on load identification [3, 4, 5, 6, 7], building classification and occupancy detection [8, 9], and generally all solutions targeting to make the user's environment *smarter* through the analysis of electricity consumption data [10]. While the main focus of these works

Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

is usually on the provision of novel user-oriented services, they implicitly also result in privacy issues, e.g., enabling the identification of lifestyles [11] or behavioral patterns [12].

Our key approach on enhancing user privacy is the controlled modification of the PV converter's operating point to help us obfuscate existing loads as well as to inject false load signatures into a household's aggregate consumption. As PV converters are generally equipped with MPPT algorithms, it is easily possible to retrofit them with our solution and thus make them tools for a better protection of user privacy in smart grids. We make the following contributions in this work:

- We highlight threats to user privacy resulting from the disclosure of smart meter data, as well as surveying existing means to mitigate these issues.
- We present conceptual and technical details about our modified MPPT algorithm, which allows the external control of the converter's power point in order to inject load signatures into a household's aggregate consumption.
- We evaluate how our algorithm responds to requested power changes when generating fake load signatures as well as when hiding the operation of an appliance.

This paper is structured as follows. We introduce privacy threats resulting from the disclosure of unprocessed smart meter data in Sec. II, along with a discussion of related work. Subsequently, we outline our contribution in more detail in Sec. III and evaluate its accuracy and response times in Sec. IV. Finally, we conclude this paper in Sec. V.

II. Privacy Threats and Related Work

Along with the increasingly ubiquitous online connectivity and the manifold opportunities enabled through connecting objects to the Internet, the societal awareness for privacy has grown measurably in the past years [13].

A. Privacy Threats of Smart Metering

While the secure transmission of meter readings has already been enforced at early deployment stages of smart meters [14], no such provisions exist for maintaining user privacy. In fact, technical means to ensure that collected data are exclusively used for billing are absent; today, customers need to trust their utility company to maintain the confidentiality of collected data and not release them to untrusted parties. The availability of consumption data collected by means of smart meters leads to numerous threats to user privacy. The most prominent threat results from the emergence of *Non-Intrusive Load Monitoring* (NILM) more than two decades ago [15]. This landmark idea of disaggregating household energy consumption into individual contributions has evolved into a widely addressed research challenge, and numerous researchers have presented methods to extract the presence as well as operational times of individual appliances from a home's aggregate consumption [3, 4]. However, consumption data needs to be considered highly sensitive, as it paves the way for targeted advertisement (e.g., informing customers about inefficient appliances), user profiling and household classification [8], and many others.

B. Existing Protection Approaches

The vast majority of current works on protecting user privacy in smart grids either focuses on security-enhanced data transmission solutions (i.e., applying information security solutions to transfer readings to an assumed trustworthy utility company) or collaborative approaches to exchange meter readings between different customers [16, 17]. In such approaches, values aggregated across different homes are often being used to achieve k-anonymity, i.e., the unlinkability between appliance operation and the actual dwelling (out of the k potential ones) in which it has taken place. Other solutions to tackle this issue can generally be categorized as (1) the anonymization of meter data [18], (2) the privacy-preserving aggregation of meter data [19], and (3) the masking and obfuscation of meter data [20, 21]. This work is concentrating on the latter category, and we hence discuss existing works in the domain of load hiding as follows.

Solutions for the obfuscation and masking of meter data can be divided into load hiding using a battery and load hiding based on controllable loads. A battery-based load hiding system charges and discharges a battery at strategic times to flatten the household's energy demand. Ideally, all rapid changes in power demand should be covered by the battery to flatten the energy consumption observed by the smart meter [22], and thus obfuscate characteristic consumption patterns which can be used to infer user and/or appliance activity. Several algorithms have been proposed in the field of battery-based load hiding in [20], such as non-intrusive load leveling (NILL) and the stepping framework.

In contrast to battery-based approaches, load hiding techniques can also employ dedicated appliances with large power consumption, such as a water boiler, to obfuscate the power demand. One such approach towards load-based load hiding is presented in [7]. To protect user privacy, the water boiler is randomly turning on and off with the constraint to meet a given daily power consumption. This addition of noise to the overall household power demand has been shown to strongly decrease the success rate of NILM algorithms. Another work [23] uses a thermal energy storage of large elastic heating loads to fake power profiles of other appliances in homes. This technique does not aim to prevent against load disaggregation techniques, but instead tries to inject the load profiles of typical home activities into the aggregate consumption. Accordingly, it successfully prevents occupancy detection techniques [9].

C. Comparing our Approach to Existing Work

Our work differs from related work in two main regards: Firstly, all existing load hiding approaches rely on adding electrical devices (e.g., a water boiler or a battery) to consume power on demand. This implies a monetary cost to purchase, install, and maintain these devices. Our approach relies on a device that is already present in domestic PV installations and thus alleviates this burden. Secondly, existing approaches generally intentionally consume power (e.g., by activating a water boiler) or convert it to different types of energy (e.g., chemical energy stored in a battery) which entails conversion

Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

losses, often radiated in the form of thermal energy. Our solution instead modifies the PV converter such that power is not being generated in the first place. As our proposed deviation from the MPP does not lead to any (mechanical or electrical) degradation of the PV panels or the power electronics in PV converters, the solution has no negative technical side effects.

III. Concept and Implementation

The core idea of our work is to intentionally lower (or raise) photovoltaic generation in order to create signatures in a household's aggregate power consumption which did not originate from the actual operation of electrical appliances. Controlling a converter's MPPT algorithm can be used to intentionally deviate from the MPP, and thus represents a viable basis for realizing our concept. Moreover, PV generation curtailment directed by utilities has also been proposed to deal with voltage rise issues in distribution networks with high PV penetration [24].

A. Conceptual Considerations

Our system design is driven by two main applications, both of which can be achieved when modifying the output power of a small-scale domestic PV installation:

1) The generation of artificial appliance signatures (similar to the notion of load-based load hiding, as discussed in Sec. II-B). This approach can, e.g., be used to simulate user presence even when no persons are physically there. Besides mitigating the risk of burglaries, artificial signatures also make it harder for attackers to determine a user's typical habits and daily activities.
2) Hiding existing loads through increasing PV generation. To this end, the PV generation must be set to an output power below its maximum capacity prior to the requested operation, such that the instantaneous increase of its generation becomes possible by replaying the inverse consumption of an appliance, i.e., increasing PV generation linearly with the appliance's demand.

An important consideration to make when modifying power consumption readings is to decide whether smart meters should be allowed to report values that differ from the actual consumption. As such an approach would, however, defeat their primary purpose (i.e., billing and supporting more fine-grained capacity planning), we do not follow such a strategy. In other words, no changes are required to the smart meter as long as it reports the total aggregate consumption of a dwelling (i.e., $P_{consumed} - P_{generated}$). This, however, also implies that generation and load need to be connected to a single meter and that our approach is inapplicable when generation and load measurements are performed separately, as the unprocessed load data with all its sensitive detail is reported to the utility company in this case.

Operating a PV installation below its MPP is a necessary requirement for our load hiding approach, yet it implies that less power is converted than possible. While this can be expected to lead to lower returns from the sales of energy to the grid operator, we believe this is a reasonable monetary cost to bear as the *price of privacy*.

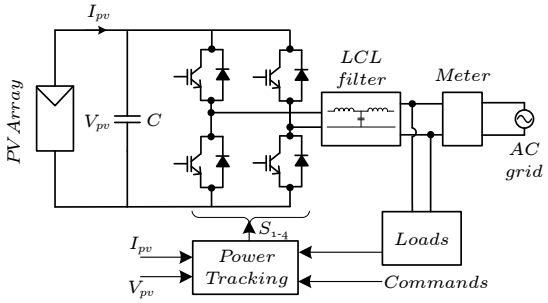


Fig. 2. Single-stage, single-phase PV inverter with the proposed power tracking control.

B. Overall Architecture and Implementation Details

MPPT algorithms are omnipresent in state-of-the-art PV converters. Their operation is based on tracking the peak of the PV curve under given irradiance and temperature conditions. It is hence mandatory for our system to know about the relation between V_{pv} and the resulting output power P in order to achieve a controlled reduction or increase in PV generation. We currently achieve such knowledge through the implementation of pre-defined lookup tables that map the relations between known irradiance and temperature values to a known power output behavior. Alternatively it would also have been possible to iteratively adjust the operating point in a closed loop until the desired change in the converter's output power has been observed. However, the limited rate of change would make it impossible to model rapid power consumption changes (which, e.g., occur when turning on a capacitive load) in the converter's output power, and we have thus decided against this approach. In the long run, we strive for a more adaptive solution, such that curves with multiple extremal values, e.g., as a result of partial shading conditions, can be appropriately modeled (cf. Fig. 3 for an example of the actual PV output on one such day).

A schematic of the single-stage, single-phase PV system used in our models and simulations is shown in Fig. 2 with the relevant system parameters given in Table I. The system consists of a single-phase full-bridge inverter connected to the ac grid through an LCL filter. The converter performs MPPT by regulating the dc voltage to the required level. Our proposed system is based on a modification of the *Incremental*

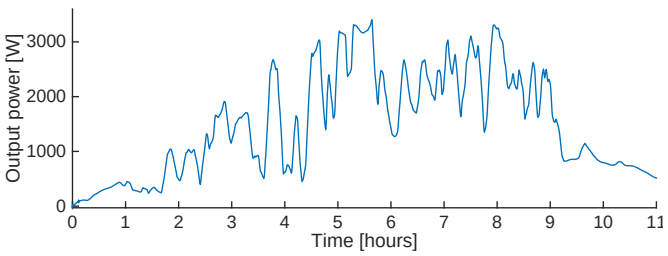


Fig. 3. Excerpt of the PV generation on a cloudy day (starting time 7.00am).

Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Grid voltage (V_g)	230 V
Grid frequency (f)	50 Hz
Switching frequency (f_{sw})	20 kHz
DC link capacitor (C)	2 mF
V_{MPP} (at 1000W/m^2)	17.6 V
I_{MPP} (at 1000W/m^2)	3.69 A
$V_{opencircuit}$ (at 1000W/m^2)	22.1 V
$I_{shortcircuit}$ (at 1000W/m^2)	3.99 A

Conductance algorithm [25], a widely used solution to realize MPPT. The main novelty of our modification relies on the addition of an external input signal to the power point tracker, such that an intentional deviation from the MPP becomes possible. In the resulting MPPT algorithm, the peak of the power is tracked by operating at the point where $dP/dV_{pv} = 0$ for the curves of Fig. 1a. In order to deviate from the MPP, we force the algorithm to operate at a point where $dP/dV_{pv} < 0$, with the exact value defined by the PV curve and the required deviation from the MPP.

It needs to be noted that the maximum output power of the PV array under given environmental conditions is the limiting factor in the injection of simulated load signatures and load hiding. More precisely, our approach can only be used during times when sufficient PV generation exists (i.e., it has limited use during occluded skies and is inapplicable during the night) to simulate or hide appliance signatures. Moreover, quickly changing environmental conditions require the parallel execution of MPPT and the forced injection of deviations from the optimum power point. In such situations, deterministically predicting the converter's response during simultaneous variations of these two input parameters remains an open challenge.

IV. Evaluation

In order to assess the performance of our solution in terms of its success of generating simulate appliance load signatures and hiding actual appliance operations.

A. Evaluation Setup

We have conducted simulations of a grid-connected PV converter with the modified MPPT algorithm using MATLAB/Simulink and PLECS. The following sections outline the simulated setup and selected result demonstrate both modes of operation. All input data were fed to the system at a resolution of 1 Hz, identical to the sampling resolution of state-of-the-art power monitors like the Plugwise [26] system. Our system includes a single-phase, single-stage PV inverter which connects the PV array to the power grid through an LCL filter. The solar array consists of two strings, each composed of 22 BP365 modules (rated at 65 W each) in series. Characteristics of the PV modules and the PV inverter are also tabulated in Table I. Tracking of the MPP is achieved by controlling the voltage of the dc-link to the required value while a linear PI controller is used for the control of the converter current.

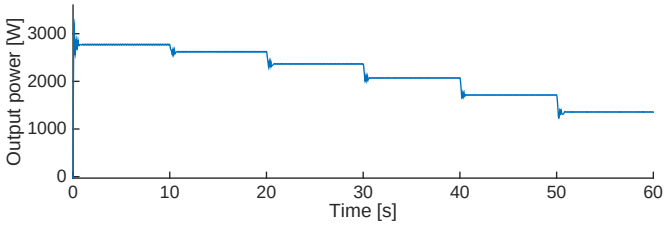


Fig. 4. Demonstration of the response times when setting the converter's desired output power (0.02 ms temporal resolution on the x-axis).

B. Controlled Power Point Shifting

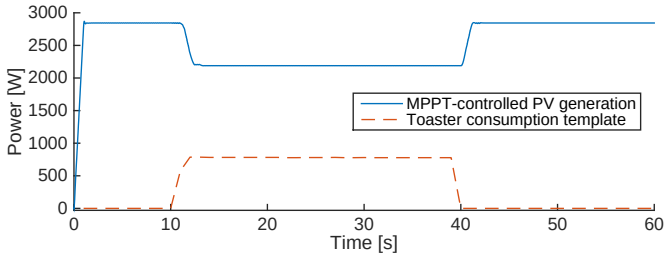
As a first result, we demonstrate how the intentional deviation from the converter's power point is reflected in its output power. To this end, we have configured the modified MPPT algorithm to stepwise reduce the converter's output power every 10 seconds; the result is visualized in Fig. 4. The diagram shows that response to the requested deviation from the MPP are almost instantaneous and mainly depend on the frequency at which MPP changes are processed. Minor oscillations are observed after each transition, which indicate a change of the converter's power point. However, their amplitudes are highly similar regardless of input and output power level, hence they do not allow an attacker to draw conclusions about whether a large or small change to the converter's output power has been requested. Both fast response times to requested output power changes and the inability to infer the amplitude of power changes are vital elements in using our approach to protect user privacy, and both of them are fulfilled.

C. Simulating Appliance Load Signatures

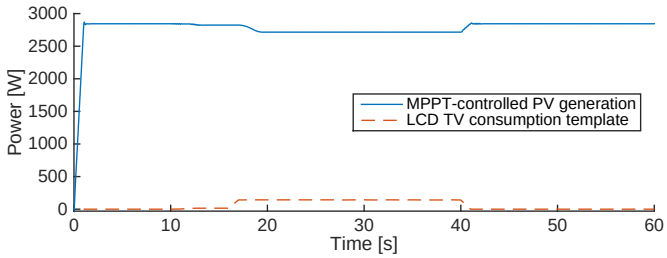
Having demonstrated the solution's ability to quickly respond to requested output power changes, we now investigate how it is able to simulate appliance signatures without these devices being operated in practice. As introduced in Sec. III-A, the first use case is based on reducing the converter's output power, and its practical use cases include pretending user presence and adding load signatures for appliances not physically owned, e.g., to confuse an attacker. In order to simulate appliance operation, the corresponding load signatures are required as inputs to our modified MPPT algorithm, and such traces have been extracted from the Tracebase data set [6]. In the following evaluations, we use both a trace for both a larger consumer (a toaster oven; 800 W peak power consumption) and a rather small appliance, namely an LCD television set with peak consumption of 150 W.

The results for simulating the load signatures of these two appliance types are shown in Fig. 6. We have set the operational duration of the appliances to 30 seconds, in order to observe the MPPT algorithm's behavior during output power transitions better. Retaining the appliance's usual operational durations (e.g., minutes or even hours for the TV) is nonetheless possible; neither the behavior during the transition times nor the one during steady-state operation change when extending the operational times.

Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

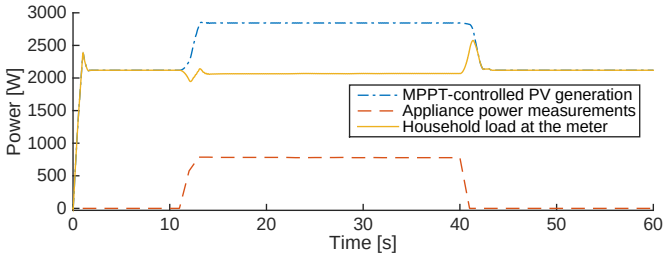


(a) Simulated toaster load signature.

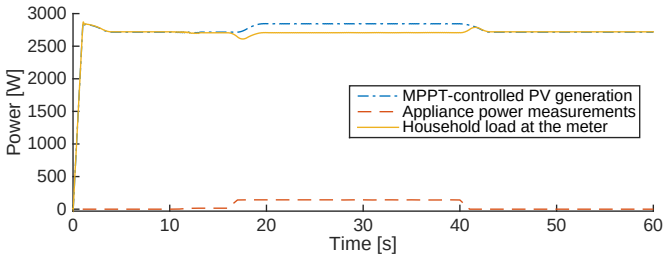


(b) Simulated LCD TV load signature.

Fig. 5. Load simulation is realized by injecting existing load signatures (e.g., from a pre-defined library) into the converter's MPPT algorithm.



(a) Hidden toaster load signature.



(b) Hidden LCD TV load signature.

Fig. 6. Load hiding is realized by injecting real-time measurements (e.g., collected by means of plug-level meters) into the converter's MPPT algorithm.

Analysis of the figures confirms that the converter's output power drops for the duration of the appliance operation, and returns to nominal level afterwards. Although an (approximately) one-second delay can be observed before the input stimulus is observed at the converter's output, this commonly does not represent a problem when simulating loads (in comparison to load hiding where instantaneous compensation of loads is highly desirable, cf. Sec. IV-D). In conclusion, our simulation results allow us to conclude that injecting load signatures into a household's aggregate load is easily possible through our proposed method. The signatures required to perform this operation can be easily extracted from previous appliance operations (e.g., by means of plug-level power sensors) or simply downloaded from publicly available data sets. In terms of monetary cost, the operation of a simulated appliance is equally expensive as the actual appliance's operation (assuming identical tariffs for generated and consumed electricity).

D. Load Hiding

In the previous evaluation, we have used our modified MPPT algorithm to simulate loads which were not present in a home. In this part, we now assess at which accuracy the second required mode of operation, namely load hiding (cf. Sec. III-A), can be performed. To realize load hiding, the converter's output power needs to be increased by the same amount as the load's consumption rises. This is vital to maintain the same household total consumption, $P_{consumed} - P_{generated}$, as before the start of the appliance activity. Assuming an instantaneous response and an accurately controllable converter output, load signatures can effectively be hidden from the household aggregate power consumption this way, and no sensitive details are released to the utility company or other third parties.

In practice, however, it is not possible to reduce all delays to zero, as the collection and transmission of appliance power consumption, as well as its processing in order to set the converter's operating point take up time. We present results of load hiding operations for the toaster and the LCD television appliances in Fig. 7, where a one-second delay can be observed between the recording of power data and its use in the PV converter's power tracking algorithm. Note that this delay dominates the load hiding accuracy, whereas the oscillations observed after transitions (cf. Fig. 4) could not be determined to measurably contribute to the latency.

In the two diagrams, the dashed line in the bottom part represents the actual consumption of the appliance, as measured by means of a plug-level meter. Assuming no load hiding was taking place, this additional consumption would be directly visible in the household aggregate load, and thus pose risks to user privacy through the use of NILM (cf. Sec. II-B). In order to alleviate these issues, our load hiding approach increases generation (through the same adaptation of the converter's power point as used before) by the same extent as the load's power draw. The dash-dotted line in the figures shows the output of the PV generation when our MPPT-based load hiding approach is being used. By increasing generation when the load increases, the resulting total consumption (the continuous line in the diagrams) does not reveal amplitude information about the underlying appliance's load signature. Instead, only very short (2–3 seconds) power spikes can be observed in the transition regions, which result from the non-zero delays between appliance load metering and the corresponding setting of the converter's power point.

As a final observation, this way of load hiding requires households to run their PV systems at a lower power in order to gain the ability to increase generation on demand. We need

Preprint of: **A. Reinhardt**, G. Konstantinou, D. Egarter, and D. Christin. "Worried About Privacy? Let Your PV Converter Cover Your Electricity Consumption Fingerprints." In: *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm) Symposium on Cyber Security and Privacy*. 2015, pp. 25–30.

to remark, however, that it is not necessary to run the PV array at sub-optimum operating points throughout an entire day. Knowledge of typical appliance operation times can be exploited to reduce PV power ahead of the expected appliance operation (e.g., by using data similar to Fig. 3 as an input to simulate appliance load signatures before the anticipated appliance operation), and thus only gain the required generation capacity when needed.

V. Conclusions

Protecting user privacy in an increasingly digital world becomes more and more important. With the mandatory deployment of smart metering infrastructure in many countries across the globe, sensitive information about activities and daily workflows is delivered to the utility company without adequate protection. We have proposed a novel way to leverage domestic PV installations to achieve privacy protection, namely by intentionally reducing the power generation in order to simulate user presence and appliance load signatures. The only price to pay when using our approach is the cost of temporarily generating less or no PV power; a small price to pay in order to prevent the release of sensitive information.

Our approach neither leads to an (electrical or mechanical) degradation of the PV panels nor of the converter, and as such can be easily deployed at large scale. Our practical evaluations have shown that the delays between setting a desired output power and the converter's reaction is almost instantaneous. Even when feeding data collected from appliance monitoring, observed delays mostly result from the transfer of power sensor readings from the appliance monitor to the converter. Overall, adaptation delays of less than 2 seconds can be achieved on average, and as such only short consumption spikes occur in the household aggregate consumption. They, however, they lack appliance-specific features and thus disaggregation, i.e., finding out from which appliance they originated, is much more complex.

References

[1] REN21, "Renewables 2014 Global Status Report," 2015, available online at http://www.ren21.net/REN21Activities/GlobalStatusReport.aspx, last access on 9 May 2015.

[2] T. Esram and P. L. Chapman, "Comparison of Photovoltaic Array Maximum Power Point Tracking Techniques," *IEEE Transactions on Energy Conversion*, vol. 22, no. 2, pp. 439–449, 2007.

[3] Y. Kim, T. Schmid, Z. M. Charbiwala, and M. B. Srivastava, "ViridiScope: Design and Implementation of a Fine Grained Power Monitoring System for Homes," in *Proceedings of the 11th International Conference on Ubiquitous Computing (Ubicomp)*, 2009, pp. 245–254.

[4] O. Parson, S. Ghosh, M. Weal, and A. Rogers, "Using Hidden Markov Models for Iterative Non-intrusive Appliance Monitoring," in *Proceedings of the Workshop on Machine Learning for Sustainability Workshop (MLSUST)*, 2011, pp. 1–4.

[5] M. Zeifman and K. Roth, "Nonintrusive Appliance Load Monitoring: Review and Outlook," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, pp. 76–84, 2011.

[6] A. Reinhardt, P. Baumann, D. Burgstahler, M. Hollick, H. Chonov, M. Werner, and R. Steinmetz, "On the Accuracy of Appliance Identification Based on Distributed Load Metering Data," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet and ICT for Sustainability (SustainIT)*, 2012, pp. 1–9.

[7] D. Egarter, C. Prokop, and W. Elmenreich, "Load Hiding of Household's Power Demand," in *Proceedings of the 5th IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 854–859.

[8] C. Beckel, L. Sadamori, and S. Santini, "Towards Automatic Classification of Private Households Using Electricity Consumption Data," in *Proceedings of the 4th ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys)*, 2012, pp. 169–176.

[9] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, "Non-intrusive Occupancy Monitoring using Smart Meters," in *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings (BuildSys)*, 2013, pp. 1–8.

[10] F. Englert, T. Schmitt, S. Kößler, A. Reinhardt, and R. Steinmetz, "How to Auto-Configure Your Smart Home? High-Resolution Power Measurements to the Rescue," in *Proceedings of the 4th International Conference on Future Energy Systems (ACM e-Energy)*, 2013, pp. 215–224.

[11] N. C. Truong, L. Tran-Thanh, E. Costanza, and S. D. Ramchurn, "Activity Prediction for Agent-based Home Energy Management," in *Proceedings of the 4th International Workshop on Agent Technologies for Energy Systems (ATES)*, 2013, pp. 1–8.

[12] A. Alhamoud, P. Xu, A. Reinhardt, F. Englert, P. Scholl, D. Böhnstedt, and R. Steinmetz, "Extracting Human Behavior Patterns from Appliance-level Power Consumption Data," in *Proceedings of the 12th European Conference on Wireless Sensor Networks (EWSN)*, 2015, pp. 52–67.

[13] T. Mendel, A. Puddephatt, B. Wagner, D. Hawtin, and N. Torres, *Global Survey on Internet Privacy and Freedom of Expression*. United Nations Educational, Scientific and Cultural Organization, 2012.

[14] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," 2010, National Institute of Standards and Technology Report NISTIR 7628.

[15] G. Hart, "Nonintrusive Appliance Load Monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[16] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin, "Smart Meter Aggregation via Secret-sharing," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security (SEGS)*, 2013, pp. 75–80.

[17] S. Finster and I. Baumgart, "Privacy-Aware Smart Metering: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1732–1745, 2014.

[18] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 238–243.

[19] F. Li, B. Luo, and P. Liu, "Secure and Privacy-preserving Information Aggregation for Smart Grids," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 28–39, 2011.

[20] W. Yang, "Minimizing Private Data Disclosures in the Smart Grid," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2012, pp. 415–427.

[21] A. Reinhardt, F. Englert, and D. Christin, "Averting the Privacy Risks of Smart Metering by Local Data Preprocessing," *Pervasive and Mobile Computing (PMC)*, vol. 16, pp. 171–183, 2015.

[22] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 232–237.

[23] D. Chen, D. Irwin, P. Shenoy, and J. Albrecht, "Combined Heat and Privacy: Preventing Occupancy Detection from Smart Meters," in *Proceedings of the 12th IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2014, pp. 208–215.

[24] E. Demirok, D. Sera, R. Teodorescu, P. Rodriguez, and U. Borup, "Evaluation of the Voltage Support Strategies for the Low Voltage Grid Connected PV Generators," in *Proceedings of the IEEE Energy Conversion Congress and Exposition (ECCE)*, 2010, pp. 710–717.

[25] K. Hussein, I. Muta, T. Hoshino, and M. Osakada, "Maximum Photovoltaic Power Tracking: An Algorithm for Rapidly Changing Atmospheric Conditions," *IEE Proceedings on Generation, Transmission and Distribution*, vol. 142, no. 1, pp. 59–64, 1995.

[26] Plugwise BV, "Plugwise - Smart Wireless Solutions for Energy Saving, Monitoring and Switching." http://www.plugwise.com, last access on 9 May 2015.